mySites.guru

# Balbooa Forms 2.4.3.4 Fixes Five Security Issues

Balbooa Forms 2.4.3.4 fixes five security issues in Joomla form attachments and PHP actions, several reachable with no login. Update from 2.4.3.3 now.

Phil E. Taylor | 29 September 2026

Balbooa released Forms 2.4.3.4 on 29 September 2026 and asked every customer to install it as soon as possible. The release note lists five security fixes in the Joomla form builder (`com_baforms`). Four are about file attachments, and the note describes three of them as reachable without logging in. The fifth goes back to the post-submission PHP action, the same feature behind a CVSS 10.0 CVE in August.

If your sites run Balbooa Forms 2.4.3.3, and most Balbooa Forms sites in the mySites.guru database do, they need this update. So does 2.4.3.2, the version everyone was told to install seven weeks ago.

## TL;DR

Update every Balbooa Forms install to **2.4.3.4**, then confirm the component reports 2.4.3.4. The flaws were reported by Sergiy Tryzhychynskyi and Łukasz Rybak, and David Jardin of the Joomla Security Strike Team coordinated the disclosure. There is no CVE or CVSS score yet. mySites.guru now flags 2.4.3.2 and 2.4.3.3 as vulnerable, and anything older was already flagged for worse.

## What Balbooa Forms 2.4.3.4 fixes

Balbooa's note is a table, not an advisory, so everything below comes from its wording. We have not diffed 2.4.3.3 against 2.4.3.4, and where we read something into the wording we say so.

| Area | What the vendor says it fixed | Login needed? |
|---|---|---|
| Auto-reply attachments | Path traversal via crafted filenames in `getFilePath()` and the email attachment routines | Not stated; auto-replies go to anonymous submitters |
| Temporary attachments | Unauthenticated cross-session deletion of temporary or stored | No, per the vendor |

| Area | What the vendor says it fixed | Login needed? |
| --- | --- | --- |
| | attachments via `removeTmpAttachment` | |
| Attachment references on submit | Unauthenticated cross-session manipulation of attachment references | No, per the vendor |
| Admin submission views | Stored cross-site scripting through original filenames and display names | Not stated; the filename comes from whoever uploads it |
| Post-submission PHP action | Escaping and sanitising of field shortcodes to prevent arbitrary code execution | Not stated |

## A path traversal into auto-reply emails

This is the one we would worry about most. Balbooa Forms can send the person who filled in a form an automatic reply, and those emails can attach files. The vendor says a crafted filename could walk out of the upload folder in `getFilePath()` and the attachment routines, and it calls the fix “LFI protection”. Our reading, which the diff would confirm or rule out, is that an anonymous visitor could get the auto-reply to attach a file from elsewhere on the server and send it to the address they typed into the form. On a Joomla site the obvious target is `configuration.php`, which holds the database password.

That only applies where a form has an auto-reply that sends attachments, so many sites are not exposed to it. You cannot tell which forms are set up that way without opening each one, and updating takes less time.

## Other visitors’ attachments

Two fixes concern the files a visitor uploads while filling in a form. Before 2.4.3.4, `removeTmpAttachment` did not check that the attachment belonged to the person asking to delete it, so anyone could delete temporary or stored attachments from other people’s sessions. The final submission step had the same gap: the attachment references sent with a form were not tied to the session that uploaded them, so an

attacker could point a submission at someone else's file. The vendor describes both as unauthenticated. Neither runs code. On a form that collects CVs, ID documents or signed paperwork, though, an attacker could delete or swap what a real applicant sent, and you would find out only when the file you needed was missing or wrong.

### Stored XSS through a filename

The original name of an uploaded file, and its display name, were shown in the administrator's submission view without HTML escaping. A filename is whatever the uploader says it is, so an anonymous visitor could plant script that runs when an administrator opens the submission. Script running in a Super User's browser can do anything that Super User can, including installing extensions.

### The PHP action, again

Balbooa Forms lets an administrator attach custom PHP to run after a form is submitted, and lets that PHP include field values through shortcodes. In August, CVE-2026-67364 showed that a shortcode fed from a URL parameter could inject code into that PHP, scored 10.0, and fixed in 2.4.3.2. This release adds "enhanced escaping, quotation handling, and strict sanitization" of those shortcodes to prevent arbitrary code execution. That suggests the August fix did not cover every way a value could break out of its quotes, though without the diff we cannot say how. As in August, it only matters on forms where an administrator has set up a PHP action, and that is a minority.

## Which Balbooa Forms sites are affected?

Balbooa publishes no affected range and tells everyone to update. mySites.guru now flags **2.4.3.2 and 2.4.3.3**, the two versions nothing else covered. Older releases were already flagged for earlier flaws, including CVE-2026-65880 and CVE-2026-67364, both unauthenticated remote code execution scored 10.0, so this release adds nothing to their risk. They need the same update.

**6 in 10**

Balbooa Forms installs on 2.4.3.2 or 2.4.3.3

Flagged today for this release

**1 in 6**

Already on 2.4.3.4

The release is hours old

**1 in 5**

Still below 2.4.3.2

Exposed to the CVSS 10.0 flaws

Share of Balbooa Forms component installs in the mySites.guru database, 29 September 2026.

Most sites that were two or three releases behind in August are now on 2.4.3.3, so their owners do update when told. The worry is the other end: one Balbooa Forms site in five is still on a version with a known unauthenticated remote code execution flaw, several releases after the fix and well after the July zero-day was being exploited.

## What to do now

1. **Update Balbooa Forms to 2.4.3.4** on every Joomla site that runs it, through Joomla's update manager or the mySites.guru mass updater.
2. **Check the version afterwards.** Open System, Manage, Extensions and confirm the Balbooa Forms component, not only the package, reads 2.4.3.4.
3. **Look at your forms' auto-replies.** If a form sends attachments in its auto-reply and a site stayed on an older version for a while, consider changing the database password in `configuration.php` and your hosting control panel, because that is the file a path traversal would go after.
4. **Check for administrator accounts you did not create**, since the stored XSS and the older flaws both lead to admin access.

**Still below 2.4.3.2?**

Those sites are exposed to the two unauthenticated remote code execution flaws from July and August, not only to this release. Update them first, then check them for PHP files in `images/baforms/` and anything else under `images/` you do not recognise. The original Balbooa Forms post covers what to look for.

## Six Balbooa Forms security releases since July

This is the sixth security-related Balbooa Forms release in under three months:

| Version | Date | What it fixed |
|---|---|---|
| 2.4.1 | 9 July | Unauthenticated file upload to RCE, CVE-2026-56291, which we found being exploited |
| 2.4.3 | 28 July | Unauthenticated RCE through the Signature field, CVE-2026-65880 |
| 2.4.3.1 | 31 July | Administrator-area hardening |
| 2.4.3.2 | 18 August | Released as hardening, then published as CVE-2026-67364 (PHP code injection, 10.0) and CVE-2026-67363 (payment amount tampering) |
| 2.4.3.3 | not stated | Balbooa published no security note for this release |
| 2.4.3.4 | 29 September | The five fixes above |

There are two ways to read that list. The pessimistic reading is that a form builder that takes file uploads, runs PHP and handles payments from anonymous visitors has a lot of attack surface, and outside researchers keep finding more of it. The fairer one is that Balbooa ships fixes quickly, credits its reporters, emails its customers and coordinates with the Joomla Security Strike Team. For a site owner both lead to the same place: Balbooa Forms is an extension you keep on the current release all the time, not once a quarter.

Sergiy Tryzhychynskyi was also credited on the August hardening release, and Łukasz Rybak reported the Sourcerer PHP execution flaw in Regular Labs' extension, so Balbooa Forms now has experienced researchers looking at it.

## How do I find every Balbooa Forms site I manage?

The hard part of an extension release is rarely the update. It is knowing which of your sites run the extension and which version each one is on. Past a dozen sites, logging in to each Joomla admin to check is how an install gets missed, and a missed install is how one site in five ends up still exposed to a July flaw at the end of September.

mySites.guru keeps a live inventory of the extensions on each connected Joomla and WordPress site. Search for Balbooa Forms once and you get each site running it with its installed version. The 2.4.3.4 rule is already in our vulnerability database, so connected sites on 2.4.3.2 or 2.4.3.3 are flagged on your dashboard now, and the mass updater pushes the update to all of them from one screen.

The same subscription covers the checks that matter after a flaw like this: the audit looks for PHP files in upload folders, new administrator accounts and modified core files on every site, and flags them before a customer notices. It is all part of the subscription, with no add-ons.

If a Balbooa Forms site has already been hit, fix.mySites.guru cleans it, updates it and audits it for backdoors for a single fixed fee, usually the same day.

## Severity and CVE status

Balbooa gives no severity score. Our own assessment for 2.4.3.2 and 2.4.3.3 is **High**. The attachment flaws need no login and the path traversal could expose server files, but the most serious outcomes depend on how each form is set up (an auto-reply with attachments, or a PHP action), and we have not confirmed the details in the code. If a CVE record is published with a different range or score, we will update the rule and this post to match.

Credit for the findings goes to Sergiy Tryzhychynskyi and Łukasz Rybak, and to David Jardin of the Joomla Security Strike Team for coordinating, per Balbooa's release note. We did not find these issues.

---

## Further Reading

- Balbooa: Forms 2.4.3.4 Security Hardening - the vendor's release note and the only source for the five fixes.
- Balbooa Forms Fixes an Unauthenticated File Upload RCE - the July zero-day we found, and the full run of releases since.
- Blind SQL Injection in Gridbox's Blog Author - Balbooa's page builder, fixed a week earlier.
- Sourcerer 14 and 15 did not fix CVE-2026-74253 - a Regular Labs flaw also reported by Łukasz Rybak.
- CWE-22: Path Traversal and CWE-79: Cross-site Scripting - the weakness classes behind two of the fixes.

## Frequently Asked Questions

**What does Balbooa Forms 2.4.3.4 fix?**

Five security issues, per Balbooa's own release note: a path traversal in the way uploaded files are attached to auto-reply emails, unauthenticated deletion of other visitors' attachments, unauthenticated tampering with attachment references when a form is submitted, stored cross-site scripting through uploaded filenames shown to administrators, and more escaping for field shortcodes inside the optional post-submission PHP action. Sergiy Tryzhychynskyi and Łukasz Rybak reported them, and the Joomla Security Strike Team coordinated the disclosure.

**Which Balbooa Forms versions are affected?**

Balbooa tells every installation to update to 2.4.3.4 and publishes no affected range. mySites.guru flags 2.4.3.2 and 2.4.3.3 for this release. Anything older than 2.4.3.2 is already flagged for earlier and more serious Balbooa Forms flaws, including two remote code execution issues scored CVSS 10.0, and needs the same update.

**Is there a CVE for Balbooa Forms 2.4.3.4?**

Not yet. Balbooa published no CVE, CVSS score or affected range. The disclosure was coordinated by the Joomla Security Strike Team, and the Joomla CNA has issued CVEs for earlier Balbooa Forms releases, so records may follow. If they do, mySites.guru will map them to the same rule.

**I updated to 2.4.3.2 in August. Am I safe?**

No. 2.4.3.2 fixed the two August CVEs, but it is below 2.4.3.4, and so is 2.4.3.3. Update again, then open System, Manage, Extensions on the site and check the Balbooa Forms component reads 2.4.3.4.

**How do I update Balbooa Forms on many Joomla sites at once?**

Search the mySites.guru extension inventory for Balbooa Forms to list every connected site running it with its version, then push 2.4.3.4 to all of them with the mass updater. Sites still below 2.4.3.4 are flagged on your dashboard until they are updated.

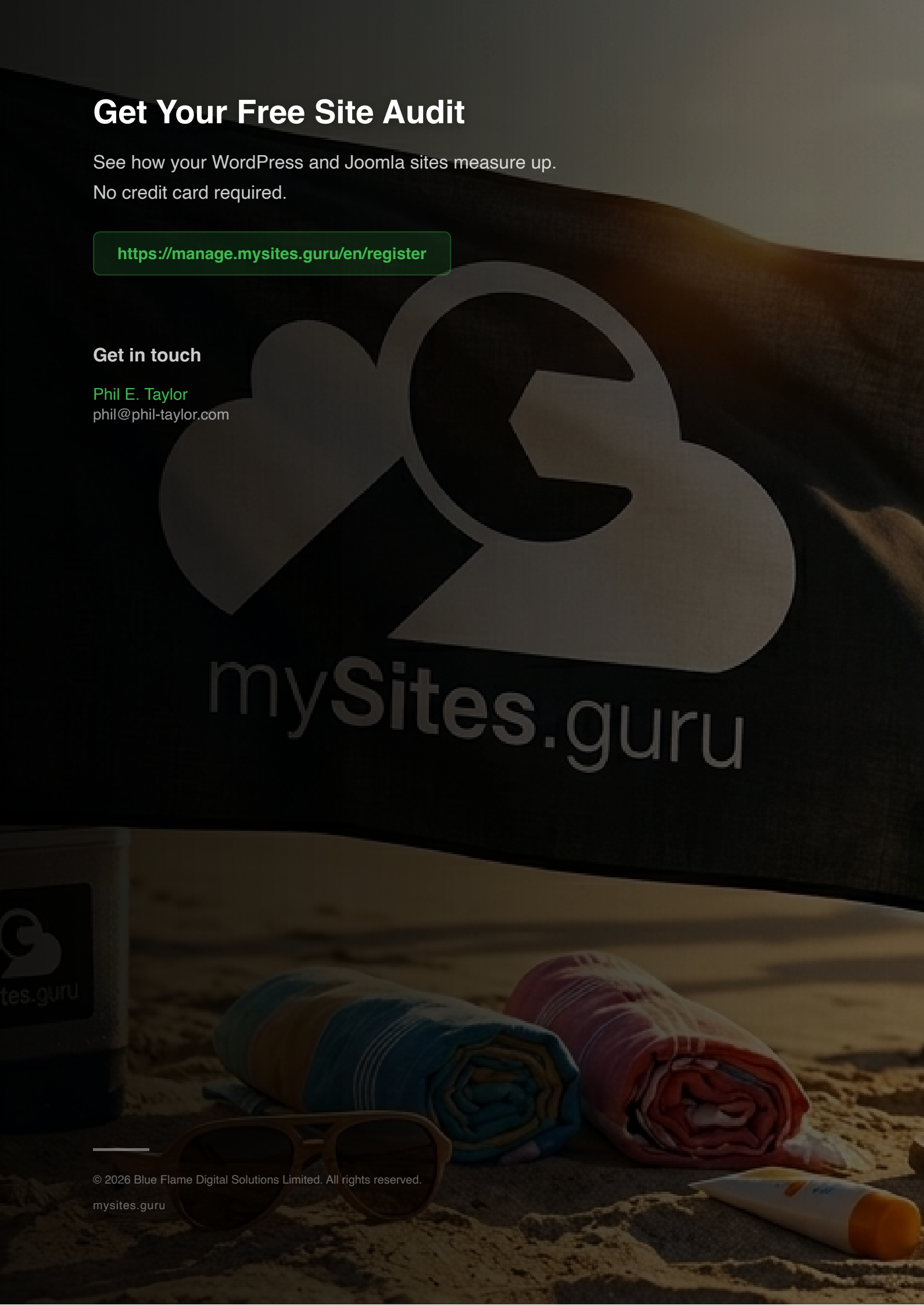

Written and edited by a human, with AI assistance. Our approach to AI

# Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

**https://manage.mysites.guru/en/register**




### Get in touch

Phil E. Taylor
phil@phil-taylor.com